

13 FEBRUARY 2004



*Communications and Information*

**CLASSIFIED MESSAGE INCIDENT PROGRAM**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: HQ PACAF/SCNI  
(Lt Col Helen M. Lento)

Certified by: HQ PACAF/SCN  
(Col Joyce R. Jenkins-Harden)

Pages: 21  
Distribution: F

---

**This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*.** It establishes the Pacific Air Forces' Classified Message Incident Program and provides policy direction to promote information assurance of the Pacific Air Forces (PACAF) Enterprise Network. This instruction does not apply to Air National Guard (ANG) or Air Force Reserve Command (AFRC) NCCs. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule*. The reporting requirements in this publication (paragraphs **2.14** and **3.3.1**.) are exempt from licensing in accordance with AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*, paragraph 2.11.5. Send comments and suggested improvements to this publication on an AF Form 847, **Recommendation for Change of Publication**, to HQ PACAF/SCNI, 25 E Street, Suite C-202, Hickam AFB, HI 96853.

- |    |                                 |   |
|----|---------------------------------|---|
| 1. | Purpose. ....                   | 3 |
| 2. | Responsibilities. ....          | 3 |
| 3. | Process Flow Walk-Through: .... | 4 |

**Attachment 1—ASSESSMENT PHASE** **8**

**Attachment 2—PROCESS DIAGRAM OF CONTAINMENT PHASE** **9**

**Attachment 3—PROCESS DIAGRAM OF SANITIZATION PHASE** **10**

**Attachment 4—PROCESS DIAGRAM OF INVESTIGATION AND  
NOTIFICATION PHASE** **11**

<b>Attachment 5—PACAF NIPRNET EXCHANGE SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)</b>	<b>12</b>
<b>Attachment 6—PACAF NIPRNET FILE/WEB SERVER SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)</b>	<b>15</b>
<b>Attachment 7—PACAF SIPRNET SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)</b>	<b>18</b>
<b>Attachment 8—PACAF SIPRNET FILE/WEB SERVER SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)</b>	<b>21</b>

**1. Purpose.** The objective of this instruction is to formalize and standardize the process to minimize the impact of classified message incidents to the network while protecting information. This program supports the following: Air Force Policy Directive 33-2, *Air Force Information Protection Program*, Air Force System Security Instruction 5020, *Remanence Security*, Air Force System Security Instruction 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting* and AFI 31-401, *Information Security Program Management*. This PACAF Instruction provides a four-phase approach to Classified Message Incidents (CMIs) and establishes an operational risk management decision matrix to assist the Designated Approval Authority (DAA) in selecting an appropriate sanitization level. IAW *DOD 5200.1-R, Information Security Program*, Chapter 10, it is Air Force policy that security incidents will be thoroughly investigated to minimize any possible damage to national security. The investigation will identify appropriate corrective actions that will be immediately implemented to prevent future security incidents. Further, if the security incident leads to the actual or probable compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.

## **2. Responsibilities.**

**2.1. Identifier:** Identifies classification of information based on proof researched during assessment phase. Contact the Wing Information Assurance Office (WIAO) for assistance as needed.

**2.2. Workgroup Manager (WM):** Notifies Network Control Center (NCC) of classified message incident and forwards his or her classification proof to NCC. WM performs initial containment of all affected workstations within his or her span of control. WM may be recalled after hours to work CMIs.

**2.3. Information Systems Security Officer (ISSO) (formerly the Unit COMPUSEC Manager):** Is the single liaison between the unit and the Information Systems Security Manager (ISSM) or WIAO for COMPUSEC matters (these duties could be accomplished by the workgroup manager). Ensures information systems are cleared or sanitized IAW AFSSI 5020.

**2.4. Unit Security Managers:** Recipient's unit security manager works with originator's unit security manager to ensure completion of inquiry/investigation. Originator's unit security manager sends final inquiry/investigation report to their Communications Squadron Commander (CS/CC) and PACAF/ SCNI, and PACAF/SF.

**2.5. Security Forces Unit:** Provides oversight and monitors the status of security incidents. IAW AFI 31-401, coordinates all security deviations involving automated information systems with the local Information Security Program Manager (ISPM) and computer security personnel to begin an evaluation on the impact of the incident to national security and the organization's operations. If communication security (COMSEC) material is involved, refer to AFI 33-212, *Reporting COMSEC Deviations*.

**2.6. Information Security Program Manager (ISPM):** The Director of Security Forces, Pacific Air Forces, is the command Information Security Program Manager (ISPM). The senior security forces official at each PACAF installation serves as the ISPM for that installation. The ISPM manages information, personnel, and industrial security programs for the activities they serve. The ISPM manages Information Security Program implementation, provides oversight within their jurisdiction and provides and monitors training IAW Chapter 8 of AFI 31-401.

2.7. **NCC:** Acts as focal point for cradle-to-grave actions for CMI. NCC will maintain file of WM appointment letters with after hours contact information/procedures. **NOTE:** Instead of WM appointment letters, Unit CCs may provide alternate recall instructions (e.g. 24 hr workcenter, job control function, etc).

2.8. **PACAF Network Operations & Security Center (NOSC):** Gathers details of the CMI from the NCC. PACAF NOSC is responsible for overall tracking and reporting of CMIs.

2.9. **CS/CC or senior communicator:** Provides command and control and interface up chain of command. Prepares OPREP, as necessary, for WG/CP concerning interruption of the information operations environment.

2.10. **Wing Commander/Designated Approval Authority (Wing CC/DAA):** Applies operational risk management (ORM) based on [Attachment 5](#) thru [Attachment 8](#) to determine appropriate sanitization level.

2.11. **WG/CP:** Receives and elevates OPREP/information from the CMI.

2.12. **Wing Information Assurance Office (WIAO):** Provides oversight and monitors the status of sanitization efforts. Also assists users in verifying incident classification.

2.13. **PACAF/SCNI:** Provide CMI Information Assurance (IA) Metric monthly briefing slides to PACAF/SC.

2.14. **PACAF/SC:** Briefs CMI IA metric monthly to COMPACAF.

2.15. **PACAF/SFI:** Provides oversight to security investigation process.

### 3. Process Flow Walk-Through:

3.1. **ASSESSMENT PHASE** (See [Attachment 1](#) for process diagram of Assessment Phase):

3.1.1. Individual initially identifying the information as classified (identifier) immediately notifies WM. Identifier should contact the ISSO or NCC rep if a WM is unavailable.

3.1.2. WM (or ISSO, NCC rep) physically disconnects the identifier's system from the network and secures system until sanitization is complete.

3.1.3. The identifier, working with the WIAO as needed, identifies classification proof. Proof of classification can be paragraph reference to source document, classification guide, or confirmation of an original classification authority (OCA).

3.1.4. The identifier's system will be reconnected to the network if it is determined that the information is not classified.

3.1.5. WM (or ISSO, NCC rep) notified by recipient (identifier) of proven classified information. WM (or ISSO, NCC rep) records contact information of individual making notification.

3.1.6. WM (or ISSO, NCC rep) notifies unit security manager and chain of command with all pertinent data including level of infection/impact. IAW AFSSI 5021, all details of a CMI are classified until the system(s) involved is sanitized. Ensure method of notification uses the proper level of security.

3.1.7. WM (or ISSO, NCC rep) notifies NCC of incident and forwards proof of classification received from the individual reporting the incident to the Network Control Center (NCC). NCC labels event as a CMI.

3.1.8. Recipient's security manager works with originator's security manager to ensure an inquiry/ investigation is conducted IAW AFI 31-401, *Information Security Program Management*, paragraph 9.3, to determine if classified information was compromised. The originator's security manager will notify his or her servicing Security Forces Squadron (or PACAF/SFI if CMI takes place in Headquarters PACAF) by the end of the first duty day that he or she became aware of the incident. The ISPM will coordinate with the organization security manager to ensure the commander has been briefed on the incident. The ISPM will brief the commander if the security manager is unable to do so or when the incident is reported directly to the ISPM.

3.2. **CONTAINMENT PHASE** (See [Attachment 2](#) for process diagram of Containment Phase):

3.2.1. WM (or ISSO, NCC rep) disconnects all affected workstations within his or her span of control from the network.

3.2.2. NCC locks user accounts of all CMI recipients. If classified information resides on a file or web server, the NCC will isolate these devices from the network.

3.2.3. NCC provides initial CMI report to the PACAF NOSC IAW AFSSI 5021, Attachment 8, paragraph A8.2. Classify reports IAW AFSSI 5021, para 3.8.8.1. Forward, via SIPRNET, a copy of the actual message involved in the CMI (e.g., email message, email message with attachment, copy of the information from the web page where classified information is posted, or DMS/AUTODIN message) to the PACAF NOSC. **Do not forward TOP SECRET or SCI information.**

3.2.4. PACAF NOSC provides CMI report to PACAF/SCNI via SIPRNET. **Do not forward TOP SECRET or SCI information.**

3.3. **SANITIZATION PHASE** (See [Attachment 3](#) for process diagram of Sanitization Phase):

3.3.1. CS/CC is OPR for building sanitization COA. NCC recommends sanitization level, based on information obtained from WM reporting the incident and the CMI Sanitization Matrix at [Attachment 5](#) thru [Attachment 8](#) as appropriate, to the Information Systems Flight Commander and the CS/CC.

3.3.2. CS/CC recommends sanitization course of action (COA) to the Wing DAA.

3.3.3. Wing DAA, weighing mission requirements against risk of compromise, applies careful ORM based on appropriate Sanitization Matrix at [Attachment 5](#) thru [Attachment 8](#) and directs appropriate sanitization level. The Wing DAA may direct a lower sanitization level than the level recommended by CS/CC based on sensitivity of information or impact on mission operations.

3.3.4. CS/CC prepares an OPREP, as necessary, for information service interruption IAW AFMAN 10-206.

3.3.5. NCC submits an updated CMI report, (to include the Wing DAA approved sanitization COA) to the PACAF NOSC.

3.3.6. NCC implements sanitization measures, to include measures to sanitize affected workstations. WMs must take immediate action to sanitize workstations at the level approved by Wing DAA. Label (recommend a label size of 1 ½" x 3" affixed adjacent to the model/serial number

plate of the device) sanitized workstations and network storage devices as *Classified information exceeding the level authorized written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.*

3.3.7. NCC notifies chain of command when sanitization measures are complete.

3.3.8. NCC re-enables all sanitized systems and notifies CMI recipients' WMs they may reconnect sanitized workstations.

3.3.9. NCC submits final CMI report to PACAF NOSC IAW AFSSI 5021, Attachment 8.

**3.4. INVESTIGATION AND NOTIFICATION PHASE** (See [Attachment 4](#) for process diagram of Investigation and Notification Phase).

3.4.1. Investigating officials will be briefed on their investigative duties by the ISPM. Completed reports will be reviewed by the ISPM for technical completeness and by the Staff Judge Advocate for any disciplinary actions contemplated. A detailed examination of evidence to determine the extent and seriousness of the compromise of classified information is required. The formal investigation will fix responsibility for any disregard (deliberate or inadvertent) of governing directives that led to the security incident.

3.4.1.1. The commander or staff agency chief of the activity responsible for the security incident will appoint an investigative official to conduct an investigation.

3.4.1.2. The formal investigation may be initiated without a preliminary inquiry if it is deemed prudent

due to the seriousness of the security incident.

3.4.1.3. The formal investigation will include the preliminary inquiry if one has been conducted.

3.4.2. PACAF NOSC takes all CMI reports and gathers all pertinent information for each event.

3.4.3. Pertinent information for this notification includes:

3.4.3.1. CMI originator's unit and office symbol.

3.4.3.2. CMI originator's host Wing Commander or equivalent; specifically:

3.4.3.2.1. For tenant organizations on an Air Force installation, identify the host Wing Commander.

3.4.3.2.2. For non-AF organizations, identify the unit and office symbol for the first O-6 equivalent in the chain of command of the CMI originator.

3.4.3.2.3. For MAJCOM staff agencies, other services, unified/specified commands, or DoD staff agencies, identify the unit and office symbol for the first General Officer in the chain of command.

3.4.3.3. Downtime of servers by base (to include message transfer agents taken off line) for the purpose of sanitizing CMIs.

3.4.3.4. Total number of users impacted by base.

3.4.3.5. Total number of servers impacted by base.

3.4.3.6. Description of CMI. **NOTE:** Provide a brief description of how the information was introduced onto the network/system.

3.4.3.7. A copy of the actual message involved in the CMI (i.e. email message, email message with attachment, copy of the information from the web page where classified information is posted, or DMS/AUTODIN message). ***Do not forward TOP SECRET or SCI information.*** If this information (TS or SCI) is required, special instructions will be given.

3.4.4. The PACAF NOSC provides pertinent information from paragraph 3.4.2. to PACAF/SCNI for action.

3.4.5. CMI originator's unit security manager sends final inquiry/investigation report to CS/CC, PACAF/SCNI, and PACAF/SF.

3.4.6. PACAF/SCNI provides CMI IA Metric monthly briefing slides and investigation results to PACAF/SC.

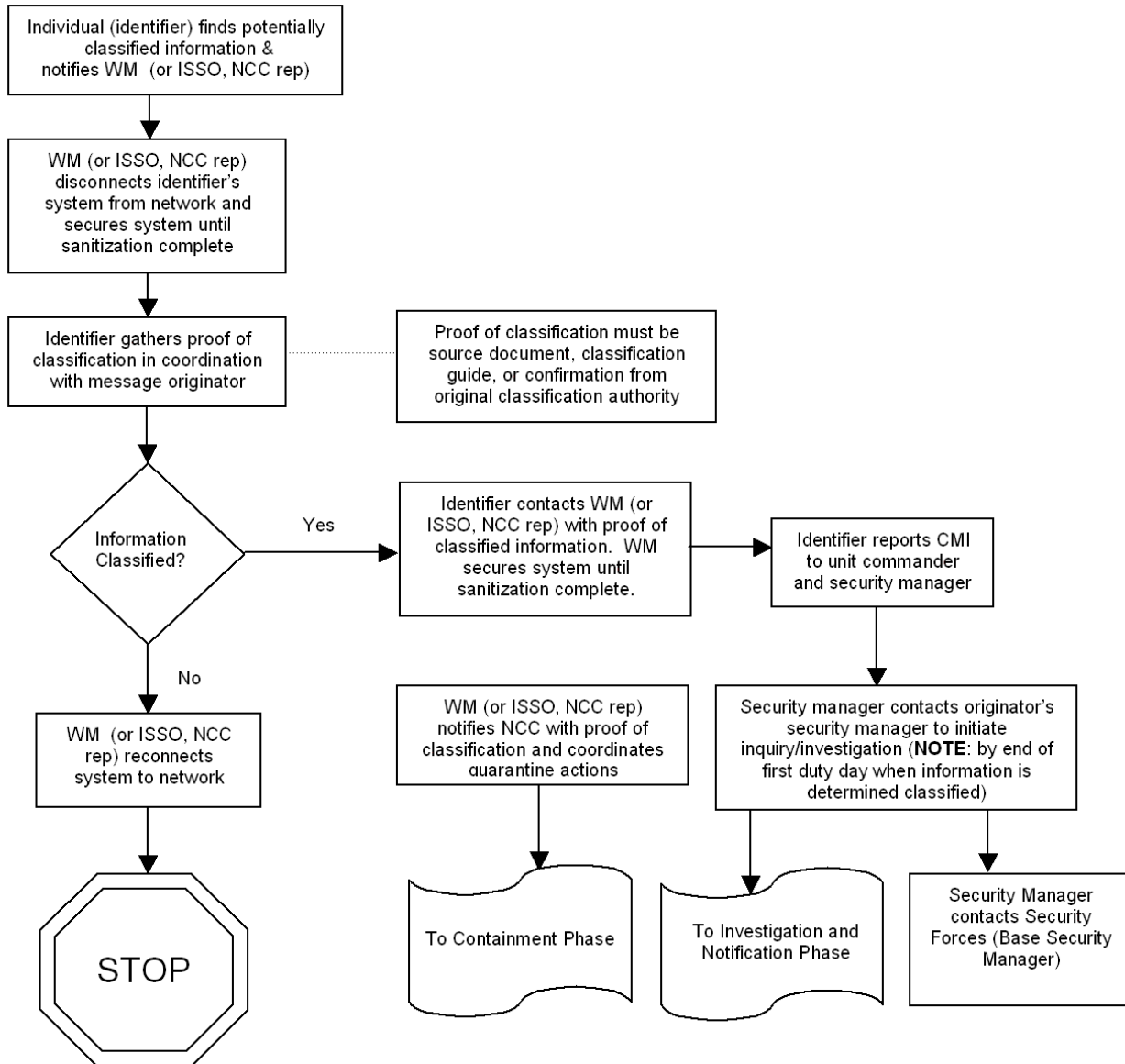
3.4.7. PACAF/SC briefs CMI IA Metric monthly to COMPACAF.

GREGORY L. BRUNDIDGE, Colonel, USAF  
Director, Communications and Information

## Attachment 1

## ASSESSMENT PHASE

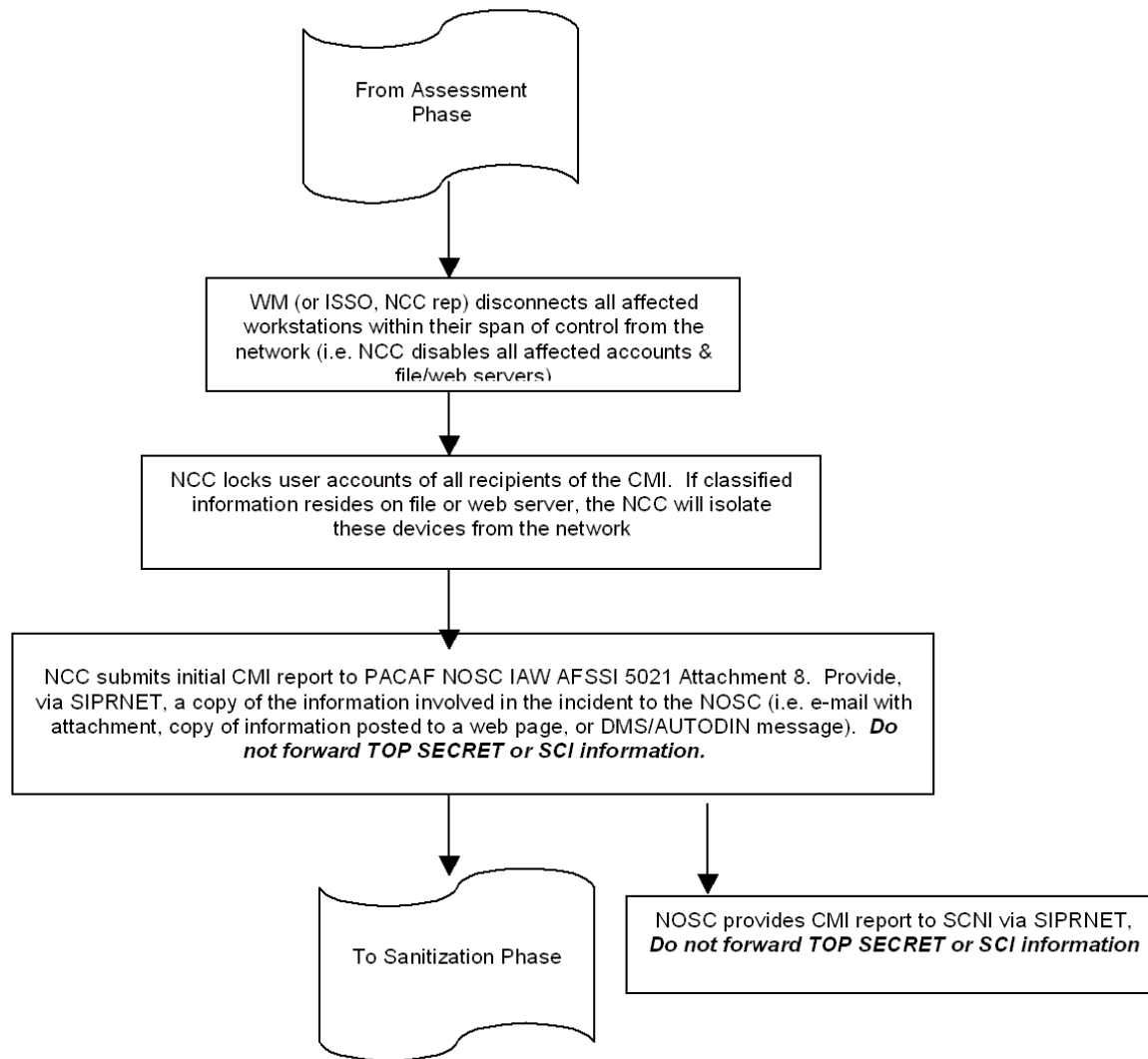
Figure A1.1. Assessment Phase.



## Attachment 2

## PROCESS DIAGRAM OF CONTAINMENT PHASE

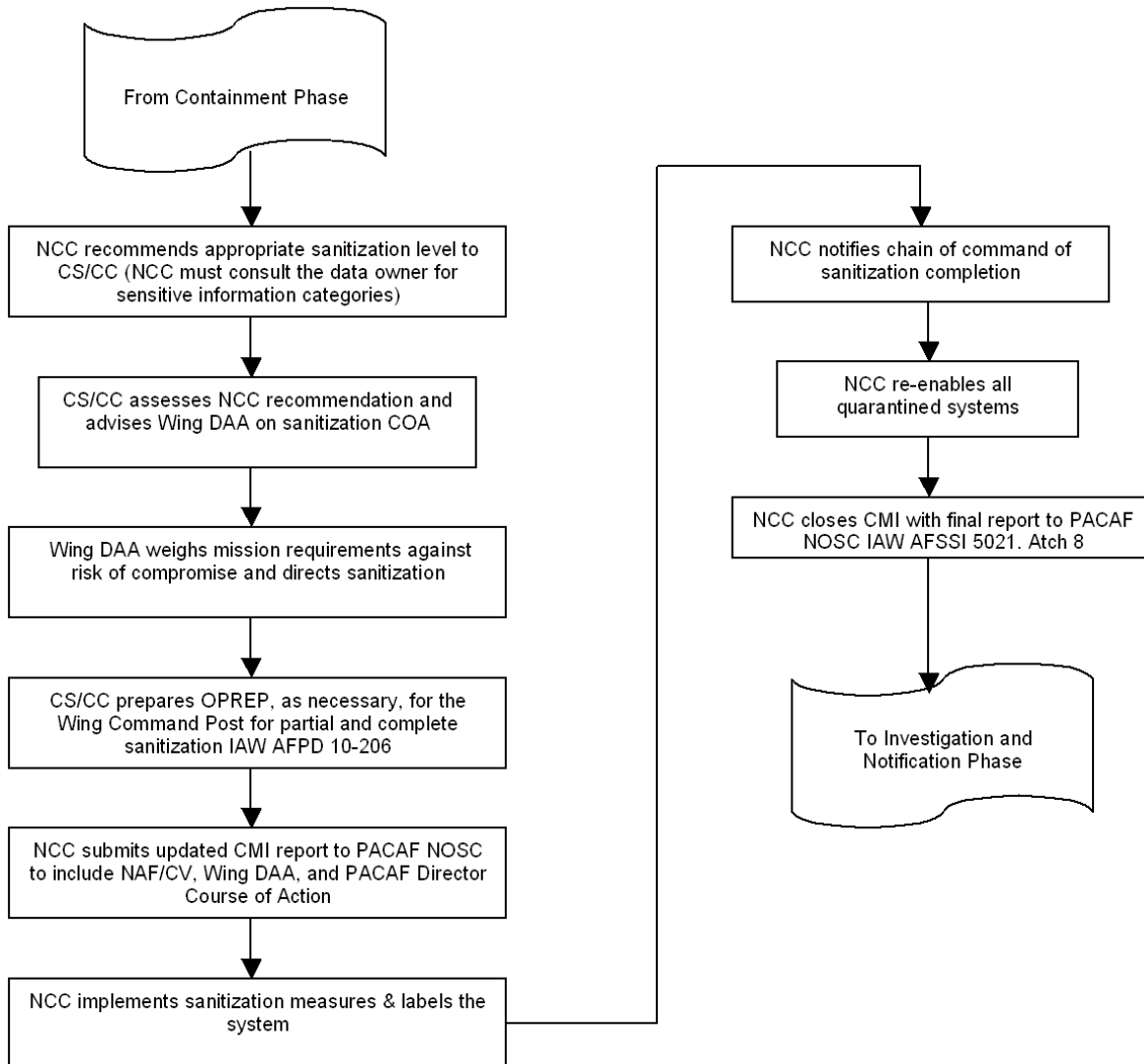
Figure A2.1. Containment Phase.



## Attachment 3

## PROCESS DIAGRAM OF SANITIZATION PHASE

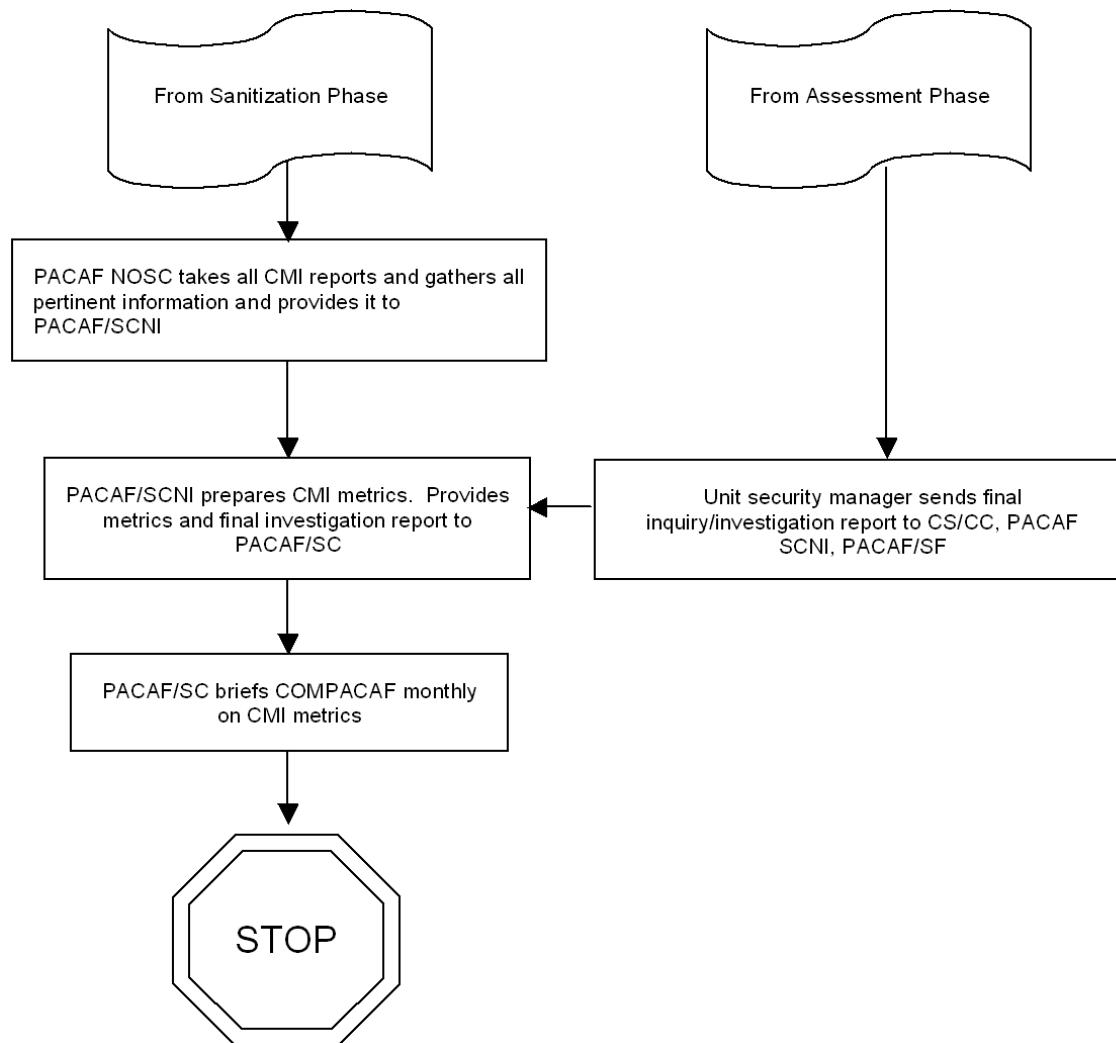
Figure A3.1. Sanitization Phase.



## Attachment 4

## PROCESS DIAGRAM OF INVESTIGATION AND NOTIFICATION PHASE

Figure A4.1. Investigative and Notification Phase.



**Attachment 5****PACAF NIPRNET EXCHANGE SANITIZATION  
OPERATIONAL RISK MANAGEMENT (ORM)**

**A5.1. NIPRNET Exchange Sanitation ORM.** The below decision matrix provides the DAA a guideline to assist with ORM in selecting a sanitization option. After applying ORM, “limited” should generally be the most common form of sanitization as it presents the most acceptable balance between risk and compromise and the cost, effort, and adverse impact on mission. Complete or partial sanitizations are indicated if one or more of the given conditions are met.

**Table A5.1. NIPRNET Exchange Sanitization ORM.**

Impact	Server Actions	Workstations		
Temporary loss of e-mail service, locked users cannot log in	Turn off Message Transfer Agents, internet mail Connectors, Information Stores (See Notes 1 & 2)	Disconnect workstations from network, lock out user accounts		
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is contractor owned and operated or outside of DoD control  2. The data owner demonstrates to DAA that partial sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Complete	Full wipe, restore backup prior to event, and label or total destruction (Note 3).	Data loss, approx. 12-24 hours to restore service	Clear, sanitize IAW AFSSI 5020, format, reload, and label (Note 3). Perform functions off-line.
1. Contaminating material is classified TOP SECRET or above  2. The data owner demonstrates to DAA that limited sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Partial	Extract and delete all messages, compress information stores, wipe free disk space, and label (Note 3)	No data loss, approx. 8-12 hours to restore service	Delete messages, compress PST file (if it exists), wipe free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Originating unit security manger notifies their servicing Security Forces Squadron by the end of the first duty day they receive notification. 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM. 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

Impact	Server Actions		Workstations	
Temporary loss of e-mail service, locked users can not log in	Turn off Message Transfer Agents, internet mail Connectors, Information Stores (See Notes 1 & 2)		Disconnect workstations from network, lock out user accounts	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is government owned and operated  2. Contaminating material is classified SECRET or CONFIDENTIAL  3. The data is perishable (i.e. automatically downgraded to unclassified after a short duration)  4. The effort, cost, and adverse operational impact of a partial sanitization is greater than the residual risk of compromise associated with a limited sanitization (Note 1)	Limited	Extract, delete all messages, and label (Note 3)	No data loss, approx. 1-4 hours to restore service	Delete messages, compress PST file (if it exists), wipe free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Originating unit security manger notifies their servicing Security Forces Squadron by the end of the first duty day they receive notification. 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM. 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

**Attachment 6****PACAF NIPRNET FILE/WEB SERVER SANITIZATION OPERATIONAL RISK  
MANAGEMENT (ORM)**

**A6.1. NIPRNET File/Web Server Sanitization ORM.** The below decision matrix provides the DAA a guideline to assist with ORM in selecting a sanitization option. After applying ORM, “limited” should generally be the most common form of sanitization as it presents the most acceptable balance between risk and compromise and the cost, effort, and adverse impact on mission. Complete or partial sanitizations are indicated if one or more of the given conditions are met.

**Table A6.1. NIPRNET File/Web Server Sanitization ORM.**

Impact	Server Actions		Workstations	
Access to files disabled	Disconnect from network (Note 2).		Disconnect workstations from network	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is contractor owned and operated or outside of DoD control  2. The data owner demonstrates to DAA that partial sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Complete	Full wipe, restore backup prior to event, and label or total destruction (Note 3).	Data loss, approx. 12-24 hours to restore service	Clear, sanitize IAW AFSSI 5020, format, reload, and label (Note 3). Perform functions off-line.
1. Contaminating material is classified TOP SECRET or above  2. The data owner demonstrates to DAA that limited sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Partial	Delete file or page, defrag, wipe free disk space, and label (Note 3)	No data loss, approx. 8-12 hours to restore service	Delete file, wipe disk free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Originating unit security manager notifies their servicing Security Forces Squadron by the end of the first duty day they receive notification. 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM. 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

Impact	Server Actions		Workstations	
Access to files disabled	Disconnect from network (Note 2).		Disconnect workstations from network	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is government owned and operated  2. Contaminating material is classified SECRET or CONFIDENTIAL  3. The data is perishable (i.e. automatically downgraded to unclassified after a short duration)  4. The effort, cost, and adverse operational impact of a partial sanitization is greater than the residual risk of compromise associated with a limited sanitization (Note 1)	Limited	Delete file, wipe free disk space, and label (Note 3)	No data loss, approx. 1-4 hours to restore service	Delete file, wipe disk free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Originating unit security manger notifies their servicing Security Forces Squadron by the end of the first duty day they receive notification. 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM. 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

**Attachment 7****PACAF SIPRNET SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)**

**A7.1. SIPRNET Exchange Sanitization ORM.** The below decision matrix provides the DAA with a guideline to assist the DAA in ORM in selecting a sanitization option. After applying ORM, “limited” should generally be the most common form of sanitization as it presents the most acceptable balance between risk and compromise and the cost, effort, and adverse impact on mission. Complete or partial sanitizations are indicated if one or more of the given conditions are met.

**Table A7.1. SIPRNET Exchange Sanitization ORM.**

Impact	Server Actions		Workstations	
Temporary loss of e-mail service, locked users cannot log in	Turn off Message Transfer Agents, internet mail connectors, Information Stores (See Notes 2)		Disconnect workstations from network, lock out user accounts	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is contractor owned and operated or outside of DoD control  2. The data owner demonstrates to DAA that partial sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Complete	Full wipe, restore backup prior to event, and label or total destruction (Note 3).	Data loss, approx. 12-24 hours to restore service	Clear, sanitize IAW AFSSI 5020, format, reload, and label (Note 3). Perform functions off-line.
The data owner demonstrates to DAA that limited sanitization fails to adequately address the potential security impact of the compromise (Note 1)	Partial	Extract and delete all messages, compress information stores, wipe free disk space, and label (Note 3)	No data loss, approx. 8-12 hours to restore service	Delete messages, compress PST file (if it exists), wipe free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Consult guidance from cognizant security authority for incidents involving sensitive information (i.e. SCI, SAR, SIOP, and NATO). 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM (i.e., reference, paragraph, etc). 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

Impact	Server Actions		Workstations	
Temporary loss of e-mail service, locked users can not log in	Turn off Message Transfer Agents, internet mail connectors, information stores (Note 2)		Disconnect workstations from Network, lock out user accounts	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is government owned and operated  2. The data is perishable (i.e. automatically downgraded to unclassified after a short duration)  3. The effort, cost, and adverse operational impact of a partial sanitization is greater than the residual risk of compromise associated with a limited sanitization (Note 1)	Limited	Extract, delete all messages, and label (Note 3)	No data loss, approx. 1-4 hours to restore service	Delete messages, compress PST file (if it exist), wipe free space, and label (Note 3). Perform functions off-line.
<b>NOTES:</b> 1. Consult guidance from cognizant security authority for incidents involving sensitive information (i.e. SCI, SAR, SIOP, and NATO). 2. Prior to server containment, proof of classification from individual reporting incident must be verified by WM (i.e., reference, paragraph, etc). 3. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				

## Attachment 8

### PACAF SIPRNET FILE/WEB SERVER SANITIZATION OPERATIONAL RISK MANAGEMENT (ORM)

**A8.1. SIPRNET File/Web Server Sanitization ORM.** The below decision matrix provides the DAA with a guideline to assist in selecting a sanitization option using ORM. After applying ORM, “complete” should generally be the most common form of sanitization as the concern for confidentiality of information is higher. It presents the most acceptable balance between risk and compromise and the cost, effort, and adverse impact on mission. Complete or partial sanitizations are indicated if one or more of the given conditions are met. Limited should not be utilized.

**Table A8.1. SIPRNET File/Web Server Sanitization ORM.**

Impact	Server Actions		Workstations	
Access to files disabled	Disconnect from network (Note 1)		Disconnect workstations from network	
Guiding Conditions	Level	Server Actions	Impact	Workstation Actions
1. System is contractor owned and operated or otherwise outside of DoD control  2. The data owner demonstrates to DAA that partial sanitization fails to adequately address the potential security impact of the compromise  3. Contaminating material is TOP SECRET or SCI	Complete	Full wipe and restore backup prior to event, and label hard drive or total destruction (Note 2)	Data loss, Approx. 12-24 hours to restore service	Clear, sanitize IAW AFSSI 5020, format, reload, and label (Note 2). Perform functions off-line.
<b>Notes:</b>  1. Prior to server containment, proof of classification from individual reporting incident must be verified by WM.  2. Label sanitized workstations and network storage devices as <i>Classified information exceeding the level authorized was written to this device. The device was sanitized on (date). Do a complete sanitization IAW AFSSI 5020 prior to release or reuse outside the organization.</i>				